Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for protecting publicly accessible network computer services from undesirable network traffic in real-time, the method comprising:

receiving network traffic including a stream of service requests destined for the publicly accessible network computer services;

generating request statistics including connection statistics and service request distributions based on the stream of service requests, the request statistics including content of the network traffic and comprising at least one of: size of a request and a reply to the request; request payload; number of fragments in the request; and request content anomalies;

analyzing the request statistics including the content of the network traffic to identify an undesirable user of the services; and

limiting or removing access of the identified undesirable user to the services to protect the services.

2. (original) The method as claimed in claim 1 wherein the undesirable network traffic includes denial of service attacks.

3. (original) The method as claimed in claim 1 wherein the network is the Internet.

4. (previously presented) The method as claimed in claim 1 further comprising generating one or more user profiles from the request statistics wherein the step of analyzing includes the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user.

5. -6. (cancelled)

7. (previously presented) The method as claimed in claim 1 wherein the network is the Internet and wherein the step of generating request statistics includes the steps of collecting and correlating Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

8. (original) The method as claimed in claim 7 wherein the step of correlating includes the step of identifying a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.

9. (currently amended) A system for protecting publicly accessible network computer services from undesirable network traffic in real-time, the system comprising:

an interface for receiving network traffic including a stream of service requests destined for the publicly accessible network computer services;

a forwarding engine for generating request statistics including connection statistics and service request distributions based on the stream of service requests, the request statistics including content of the network traffic and comprising at least one of: size of a request and a reply to the request; request payload; number of fragments in the request; and request content anomalies; and

a analysis engine in communication with the forwarding engine for analyzing the request statistics including the content of the network traffic to identify an undesirable user of the services, the forwarding engine limiting or removing access of the identified undesirable user to the services to protect the services.

10. (original) The system as claimed in claim 9 wherein the undesirable network traffic includes denial of service attacks.

11. (original) The system as claimed in claim 9 wherein the network is the Internet.

12. (previously presented) The system as claimed in claim 9 wherein the forwarding engine generates one or more user profiles from the request statistics and wherein the analysis engine compares the one or more user profiles with a predetermined profile to determine the undesirable user.

13. - 14. (cancelled)

15. (previously presented) The system as claimed in claim 9 wherein the network is the Internet and wherein the forwarding engine collects and correlates Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

16. (original) The system as claimed in claim 15 wherein the forwarding engine identifies a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.